

FIPS 140 & CC

How do they get along

Dawn Adams and Erin Connor
EWA-Canada
22 September 2010

Your Trusted Partner

- **Introduction**
- **FIPS 140 Overview**
- **Cryptography Under the CC**
- **CC SFRs in FIPS 140**
 - The FCS Class
 - FCS “Logistics Tail” SFRs
 - Selected SFRs that may apply
- **CC SARs in FIPS 140**
- **Conclusion**

- **FIPS 140 is a long-standing family of standards specifying requirements for cryptographic modules**
- **It has a well established and long-running test and validation program (1400 cryptographic modules certified since 1995)**
- **Significant evidence provided and test results compiled during FIPS 140 validation testing**
- **CC evaluation of cryptographic and related functionality replicates, and in some cases falls short, of testing under FIPS 140 for cryptographic modules**
- **A case for re-use of FIPS 140 validation results**

FIPS 140 Overview

- FIPS 140 is a prescriptive conformance standard specifying **shalls** and **shall nots** for a cryptographic module (CM)
- It defines 11 security requirements “areas” addressing both functional and assurance requirements
- It defines 4 increasing qualitative Security Levels (SLs) that may be achieved in each area
 - => Requirements for each SL address both function and assurance
- During validation testing a CM receives a rating for each applicable area identifying the SL achieved, and the overall SL rating given to the CM is the lowest of the SL ratings achieved in the applicable individual areas
- Cryptographic Module Validation Program (CMVP), a joint U.S. – Canada program run by NIST and CSE, oversees the testing and validation of modules
- Complementary Cryptographic Algorithm Validation Program (CAVP) run by NIST oversees the verification and validation of implementations of FIPS-Approved security functions (algorithms)

Your Trusted Partner

FIPS 140 Overview

	Requirement Area	Security Level 1	Security Level 2	Security Level 3	Security Level 4
1	Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
2	Cryptographic Modules Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically separated from other data ports.	
3	Roles, Services and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
4	Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
5	Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
6	Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
7	Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
		Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
8	EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
9	Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
10	Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
11	Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

FIPS 140-2 Table 1

Your Trusted Partner

- **Companion – Derived Test Requirements (DTR), analogous to the CEM:**
 - Defines methods to be used by accredited Cryptographic Module Test (CMT) labs to test whether a module conforms to the requirements
 - Details the supplementary evidence that must be provided by the module vendor to support conformance testing by labs
 - Assertions are individual requirements (“shalls”) extracted from the applicable subsection in FIPS 140-2 section 4
- **Companion – Implementation Guidance (IG), analogous to Interpretations under the CC:**
 - Provide clarifications of the CMVP
 - Provide clarifications and guidance pertaining to the DTR
 - Generally based on responses issued by NIST & CSE to questions posed by CMT labs, vendors or other interested parties
 - As for DTR, keyed to the applicable subsection in section 4 of FIPS 140-2, or as general guidance for CMVP or issues that affect multiple areas

FIPS 140 Security Policy

- **The Security Policy (SP) is a required, publicly available specification of the security rules under which the module shall operate including:**
 - security rules derived from the requirements of the standard
 - additional security rules imposed by the vendor.
- **At a minimum, the following four policies shall be specified:**
 - An identification and authentication (I&A) policy
 - All roles (users), type of authentication (Role- or Identity-based), authentication data required and strength of the authentication mechanism
 - An access control policy
 - What access does operator X, performing service Y while in role Z, have to security-relevant data item W for every service provided by the cryptographic module?
 - A physical security policy
 - Specify implemented mechanisms & required operator actions to maintain physical security
 - A security policy for mitigation of other attacks
 - Specify policy & mechanism, where applicable
- **In many ways analogous to a Security Target**

Class FCS: Cryptographic support

- **Cryptographic key management (FCS_CKM)**
 - CKM.1 Cryptographic key generation
 - CKM.2 Cryptographic key distribution
 - CKM.3 Cryptographic key access
 - CKM.4 Cryptographic key destruction
- **Cryptographic operation (FCS_COP)**
 - COP.1 Cryptographic operation
- **“Logistics Tail”:**
 - Each of the FCS class SFRs have dependencies on other SFRs that must be included in the PP/ST or justification must be provided for their being left out

FCS Class “Logistics Tail”

Row -> Col	FCS					FDP						FIA	FMT				FPT	FTP		
	CKM.1	CKM.2	CKM.3	CKM.4	COP.1	ACC.1	ACF.1	IFC.1	IFF.1	ITC.1	ITC.2	UID.1	MSA.1	MSA.3	SMF.1	SMR.1	TDC.1	ITC.1	TRP.1	
FCS_CKM.1		O1		X1	O1															
FCS_CKM.2	O1			X1						O1	O1									
FCS_CKM.3	O1			X1						O1	O1									
FCS_CKM.4	O1									O1	O1									
FCS_COP.1	O1			X1						O1	O1									
FDP_ACC.1							X3													
FDP_ACF.1						X4								X4						
FDP_IFC.1									X3											
FDP_IFF.1								X4						X4						
FDP_ITC.1						O2		O2						X2						
FDP_ITC.2						O2		O2									X2	O2	O2	
FIA_UID.1																				
FMT_MSA.1						O4		O4							X4	X4				
FMT_MSA.3													X3			X3				
FMT_SMF.1																				
FMT_SMR.1											X5									
FPT_TDC.1																				
FTP_ITC.1																				
FTP_TRP.1																				

X = Required dependency O = Optional dependency # = generation after original FCS SFR

Shading indicates option “sets”

Your Trusted Partner

- **CKM.1 Cryptographic key generation**
 - Section 4.7.2 Key Generation & 4.7.1 Random Number Generators (RNGs) for keys generated using input from an RNG
 - FIPS-Approved RNG testing and validation through CAVP required
- **CKM.2 Cryptographic key distribution**
 - Section 4.7.3 Key Establishment defines req'ts and points to Annex D for approved methods; IG 7.1 and NIST Special Pub SP800-56A also apply
 - Section 4.7.4 Key Entry and Output req'ts for secret and private keys
- **CKM.3 Cryptographic key access**
 - For keys available to users or stored within the CM
 - Section 4.3 Roles, Services and Authentication (R/S/A) defines req'ts that must be formally stated in the Access Control Policy section of the SP as indicated in Appendix C
 - Section 4.7.5 Key Storage defines req'ts for the storage of keys within the CM and methods employed must be specified in evidence documentation

- **CKM.4 Cryptographic key destruction**
 - Section 4.7.6 Key Zeroization specifies req't to provide methods to zeroize plaintext secret and private keys and critical security parameters (CSPs) within the module
- **COP.1 Cryptographic operation**
 - Section 4.7.1 req'ts for RNGs; FIPS-Approved RNGs listed in Annex C
 - FIPS-Approved security functions (cryptographic algorithms) are identified in Annex A, including:
 - Symmetric – AES, 3DES, Skipjack
 - Asymmetric – DSA, RSA, ECDSA
 - Message Authentication – 3DES MAC, CCM, CMAC, HMAC
 - Hashing – SHA-1, SHA-2 (224, 256, 384 & 512 bit)
 - Testing and validation through CAVP required for all FIPS-Approved RNGs and FIPS-Approved security functions
 - Algorithms allowed but not tested ...

- **FDP_ACC.1 Subset Access Control**
 - Section 4.3 R/S/A defines access control policy req'ts for modules
 - Appendix C req'ts for Access Control Policy specific to module to appear in SP submitted as evidence
- **FDP_ACF.1 Security attribute based access control**
 - Section 4.3.3 specifies authentication req'ts
 - Note at SL1 for R/S/A area authentication is NOT required for access to the CM
- **FDP_IFC.1 Subset information flow control**
 - Section 4.2 Ports and Interfaces specifies req'ts on information flow through the CM, including user data, and control & status information

- **FDP_IFF.1 Simple security attributes**
 - Section 4.2 specifies req'ts governing flow of data into and out of the CM, including user data, keys and CSPs, especially at higher SLs
- **FDP_ITC.1 Import of user data without security attributes**
 - Section 4.7.4 Key Entry & Output specifies req'ts that surpass FDP_ITC.1, i.e., *“the correct entity (i.e., person, group or process) to which the key is assigned”* must be associated with the key by the CM
- **FDP_ITC.2 Import of user data with security attributes**
 - Section 4.7.4 Key Entry & Output specifies that at a minimum *“the correct entity (i.e., person, group or process) to which the key is assigned”* must be associated with the key by the CM
 - Manual key entry may use an EDC
 - FPT_TDC.1, upon which this requirement depends, may not be met

- **FIA_UID.1 Timing of identification**
 - Req't met by CMs that meet SL3 or SL4 for Section 4.3 R/S/A - in advance of identification, only services that do not modify, disclose or substitute keys and CSPs, or otherwise affect security of the CM are allowed
- **FMT_MSA.1 Management of security attributes**
 - Section 4.3 specifies req'ts for management access to the CM (i.e., access to management services by role)
 - SP req'd to define Access Control policy for the CM
- **FMT_MSA.3 Static attribute initialisation**
 - Section 4.3.1 specifies a minimum of two authorised roles (*User & Crypto Officer*) that a CM must support by default
 - *Crypto Officer* performs management functions

- **FMT_SMF.1 Specification of management functions**
 - All management functions provided by the CM (i.e., *Crypto Officer* role services) must appear in the SP
- **FMT_SMR.1 Security roles**
 - Section 4.3.2 specifies a CM shall provide a minimum of two roles, *User* and *Crypto Officer*
 - SP shall identify all roles recognised by CM
- **FPT_TDC.1 Inter-TSF basic TSF data consistency**
 - FIPS 140-2 does not address “distributed” CMs or the exchange of CM data with external products, thus this requirement may not be included in a validated CM
 - If capability is included in the CM it will be tested

- **FTP_ITC.1 Inter-TSF trusted channel**
 - FIPS 140-2 does not directly address CM communications with other IT products, thus this requirement may not be met by a validated CM
 - At SL3 or SL4 secret and private keys must be encrypted when using automated methods for entry/output
- **FTP_TRP.1 Trusted path**
 - Req't met by CMs that are rated SL3 or SL4 for Section 4.7, which includes a req't for *manual input* of plaintext secret or private keys using split knowledge procedures via a trusted path

- **FDP_ACC.2 Complete access control**
 - Depends on objects defined since FIPS specifies req't only for access control for keys and CSPs
- **FDP_DAU.1 Basic data authentication**
 - If CM provides MAC or Hash capability
- **FDP_DAU.2 Data authentication with identity of Guarantor**
 - Signature verification but depends on FIA_UID.1 thus CM must be at SL3 for Section 4.3 R/S/A
- **FDP_ETC.1 Export of user data without security attributes**
 - Output of keys
- **FDP_RIP.1 Subset residual information protection**
 - Req't at SL3 for hardware CM to automatically zero plaintext keys/CSPs for maintenance mode or tamper detection

- **FIA_UAU.1 Timing of Authentication**
 - services allowed before authentication at SL2 for R/S/A but depends on FIA_UID.1 so CM may need to be SL3 for R/S/A
- **FIA_UAU.2 User authentication before any action**
 - If no services allowed before authentication at SL2 for R/S/A but depends on FIA_UID.1 so CM may need to be SL3 for R/S/A
- **FIA_UAU.6 Re-authenticating**
 - Section 4.3 requires (re-)authentication to assume a role not previously authenticated and after power off. May be necessary on a service by service basis if req'd by CM
- **FIA_UAU.7 Protected authentication feedback**
 - Section 4.3 requires that provided feedback shall not weaken the strength of authentication mechanisms
- **FIA_UID.2 User identification before any action**
 - If no services allowed before identification at SL3 for R/S/A

- **FMT_MOF.1 Management of security functions behaviour**
 - Section 4.3 req't for *Crypto Officer* role to manage the CM
- **FMT_MSA.2 Secure security attributes**
 - Key lengths for Approved security functions and key characteristics for internally generated keys
- **FMT_MTD.1 Management of TSF data**
 - Section 4.3 req't for *Crypto Officer* role to manage the CM
- **FMT_SMR.2 Restrictions on security roles**
 - Section 4.3 req'ts for *Crypto Officer* and *User* roles, and where applicable *Maintenance* role
- **FMT_SMR.3 Assuming roles**
 - Section 4.3 req't for explicit assumption of roles at SL2

- **FPT_FLS.1 Fail secure**
 - Section 4.2 req't that if error occurs then CM must enter an error state and inhibit data output until cleared
- **FPT_PHP.1 Passive detection of physical attack**
 - Section 4.5 Physical Security req't at SL2 that the CM provide evidence of tampering
- **FPT_PHP.3 Resistance to physical attack**
 - Section 4.5 Physical Security specifies at SL3 and SL4 req'ts for CM response to physical access/attack
- **FPT_TST.1 TSF Testing**
 - Section 4.9 specifies significant req'ts for Power-Up tests and Conditional tests, as well as operated initiation of tests

- **No req't in FIPS 140 but will be tested during validation if present in the CM:**
 - FIA_UAU.5 Multiple authentication mechanisms
 - FMT_MTD.2 Management of limits on TSF data
 - FMT_MTD.3 Secure TSF data
 - FMT_REV.1 Revocation
 - FMT_SAE.1 Security attribute expiration
 - FPT_PHP.2 Notification of physical attack
 - FPT_RCV.1 Manual recovery
 - FPT_RCV.2 Automated recovery
 - FPT_STM.1 Reliable time stamps

- **A few brief comments on validation requirements:**
 - CM would in most cases be a subsystem within an ITS product
 - Section 4.1 CM Specification req'ts arguably correspond to ADV_TDS.3
 - Section 4.10 Design Assurance process req'ts reflect roughly:
 - EAL 3 – 4 req'ts for ADV with Section 4.1 CM Spec
 - EAL 1, 2, 3, 4 req'ts for AGD
 - EAL 2 req'ts for ALC
 - Complete source code (HW, SW, FW) review – ADV_IMP.2
 - Detailed Security Policy review and testing
 - All specified/identified/Approved CM functionality tested
 - ATE_IND.3, except that no developer tests submitted as evidence or executed

- **Significant CC claimable functionality provided in a FIPS 140 validated CM**
- **High level product assurance for cryptographic functionality gained from validation testing through:**
 - detailed Security Policy
 - access to all source code (SW, FW, HW)
 - complete testing of all relevant functionality
- **Potential for re-use of FIPS 140 validation as part of CC evaluation with or without related validation evidence or test results**

Questions



Erin Connor
Director
+1-613-230-6067 x1214
econnor@ewa-canada.com

Your Trusted Partner